Ngày 9 tháng 4 năm 2021

Gửi bằng đường điện tử

GÓP Ý CỦA LIÊN MINH PHẦN MỀM (BSA) VỀ DỰ THẢO NGHỊ ĐỊNH VỀ BẢO VỆ DỮ LIỆU CÁ NHÂN CỦA VIỆT NAM

BSA | Liên minh Phần mềm (**BSA**)[1] xin gửi lời cảm ơn tới Bộ Công an đã tạo cơ hội để chúng tôi được đóng góp ý kiến với dự thảo *Nghị định về bảo vệ dữ liệu cá nhân* (**Dự Thảo**). BSA là tổ chức hỗ trợ hàng đầu cho ngành công nghiệp phần mềm toàn cầu trước các chính phủ và trên thị trường quốc tế. Các thành viên của BSA là những công ty sáng tạo nhất thế giới, tạo ra các giải pháp phần mềm thúc đẩy nền kinh tế.

BSA ủng hộ việc Chính phủ Việt Nam thu thập ý kiến đóng góp của các bên liên quan đối với Dự Thảo và đề xuất thành lập một cơ quan bảo vệ dữ liệu tại Việt Nam là Ủy ban Bảo vệ Dữ liệu Cá nhân (**Ủy ban BVDLCN**). Thiết lập một cơ chế quốc gia về bảo vệ dữ liệu cá nhân là một bước tiến quan trọng trong việc phát triển nền kinh tế kỹ thuật số nội địa sôi động và đổi mới, đồng thời tạo điều kiện cho các công ty Việt Nam tham gia vào nền kinh tế kỹ thuật số toàn cầu.

Bản góp ý được trình lên Bộ Công an này đưa ra các khuyến nghị về các chủ đề sau:

- Công nhận vai trò riêng biệt của bên kiểm soát dữ liệu và bên xử lý dữ liệu
- Tiết lộ dữ liệu cá nhân
- Cơ sở pháp lý để xử lý dữ liệu cá nhân
- Chuyển dữ liệu cá nhân qua biên giới
- Điều khoản về đăng ký
- Yêu cầu kỹ thuật
- Dữ liệu cá nhân nhạy cảm
- Xử phạt và bồi thường

Công nhận Vai trò Riêng biệt của Bên Kiểm soát Dữ liệu và Bên Xử lý Dữ liệu

Một khuôn khổ bảo vệ dữ liệu cá nhân toàn diện phải tạo ra các nghĩa vụ hiệu quả và có thể thực thi đối với tất cả các công ty xử lý dữ liệu cá nhân. Các nghĩa vụ này sẽ chỉ có hiệu quả trong việc bảo vệ quyền riêng tư của người dân và gây dựng niềm tin nếu chúng phản ánh cách một công ty tương tác với dữ liệu của người dùng.

---

[1] www.bsa.org

Thành viên của BSA bao gồm: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cisco, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, và Workday.

300 Beach Road
#25-08 The Concourse
Singapore 199555

P: +65 6292 2072
F: +65 6292 6369
W: bsa.org

Regional Representative Office
UEN: S97RF0005K

Việc phân biệt các công ty quyết định cách thức và lý do thu thập, sử dụng dữ liệu cá nhân (thường được gọi là "bên kiểm soát dữ liệu") và các công ty xử lý dữ liệu thay mặt cho các công ty khác (thường được gọi là "bên xử lý dữ liệu") rất quan trọng vì cả bên kiểm soát dữ liệu và bên xử lý dữ liệu đều có những vai trò quan trọng, nhưng khác biệt, trong việc bảo vệ thông tin cá nhân.

Pháp luật bảo vệ dữ liệu cá nhân trên thế giới phân biệt rõ ràng hai chủ thể này và giao cho từng chủ thể các nghĩa vụ phản ánh đúng vai trò khác nhau của mỗi bên trong việc bảo vệ dữ liệu cá nhân.[2]

Điều 2 của Dự Thảo quy định về hai chủ thể khác nhau tham gia vào hoạt động xử lý dữ liệu cá nhân — "bên xử lý dữ liệu cá nhân" và "bên thứ ba". Tuy nhiên, định nghĩa của các thuật ngữ này không phù hợp với vai trò được công nhận trên toàn cầu của bên kiểm soát dữ liệu và bên xử lý dữ liệu, mà thay vào đó, kết hợp phạm vi và trách nhiệm của hai loại chủ thể này. Điều này dẫn đến sự thiếu rõ ràng và tạo ra những thách thức đáng kể trong việc áp dụng pháp luật đối với tất cả các bên liên quan, bao gồm các chủ thể dữ liệu, các công ty xử lý thông tin cá nhân và các cơ quan quản lý nhà nước.

Theo Dự Thảo, "bên xử lý dữ liệu cá nhân" được định nghĩa là cơ quan, tổ chức hoặc cá nhân trong hoặc ngoài nước thực hiện các hoạt động xử lý dữ liệu cá nhân. Định nghĩa không được giới hạn cụ thể này không chỉ ra sự khác biệt, như được ghi nhận trong pháp luật về quyền riêng tư quốc tế, giữa các chủ thể độc lập dựa trên việc liệu họ có quyết định cách thức và lý do xử lý dữ liệu cá nhân hay không (bên kiểm soát dữ liệu) hay họ chỉ là đơn vị chỉ xử lý dữ liệu cá nhân thay mặt cho các bên khác (bên xử lý dữ liệu).

Định nghĩa về "bên thứ ba" cũng làm dấy lên những lo ngại tương tự, vì định nghĩa này cũng không phản ánh khái niệm về bên xử lý dữ liệu cá nhân và bên kiểm soát dữ liệu cá nhân. Ví dụ: mặc dù các bên thứ ba dường như có thể xử lý dữ liệu cho các bên khác, nhưng định nghĩa về bên thứ ba không chỉ rõ yêu cầu quan trọng là các bên thứ ba thực hiện xử lý "thay mặt" và "theo chỉ đạo" của chủ thể chính có quyền kiểm soát dữ liệu (bên kiểm soát dữ liệu).

Chúng tôi kiến nghị sửa đổi các định nghĩa và nghĩa vụ này trong Dự Thảo theo hai hướng:

- Thứ nhất, định nghĩa về "bên xử lý dữ liệu cá nhân" nên được sửa đổi để phù hợp với định nghĩa của bên kiểm soát dữ liệu trong pháp luật của các quốc gia khác và vai trò của chủ thể này nên được phản ánh trong các nghĩa vụ cơ bản của họ. Ví dụ: vì bên kiểm soát dữ liệu có mối quan hệ trực tiếp với các chủ thể dữ liệu, Dự Thảo nên giao trách nhiệm chính cho bên kiểm soát dữ liệu để đáp ứng nghĩa vụ bảo vệ và bảo mật dữ liệu, bao gồm, cùng với các nghĩa vụ khác, xác định cơ sở pháp lý để xử lý dữ liệu cá nhân, xin sự đồng ý của chủ thể dữ liệu khi cần thiết, và thông báo cho chủ thể dữ liệu về các sự cố dữ liệu hoặc các sự cố khác có nguy cơ gây tổn hại nghiêm trọng cho chủ thể dữ liệu. Bên kiểm soát dữ liệu cũng nên là bên có trách nhiệm thực hiện các quyền của chủ thể dữ liệu đối với dữ liệu, ví dụ như các quyền theo Điều 5 của Dự Thảo.

- Thứ hai, định nghĩa về "bên thứ ba" nên được sửa đổi để phù hợp với định nghĩa của bên xử lý dữ liệu trong pháp luật của các quốc gia khác và nghĩa vụ của họ phải phù hợp với vai trò này. Ví dụ, vì bên xử lý dữ liệu xử lý dữ liệu thay mặt cho bên kiểm soát dữ liệu, bên xử lý dữ liệu thường không có mối quan hệ trực tiếp với chủ thể dữ liệu và có thể có quyền và khả năng hạn chế trong việc truy cập vào dữ liệu đang được xử lý. Do đó, bên xử lý dữ liệu không thể trực tiếp xin sự đồng ý từ chủ thể dữ liệu, thực hiện các yêu cầu về quyền của chủ thể dữ liệu đối với dữ liệu, hoặc thông báo cho chủ thể dữ liệu khi xảy ra sự cố. Thay vào đó, trách nhiệm chính của bên xử lý dữ liệu nên là thay mặt bên kiểm soát dữ liệu xử lý dữ liệu một cách phù hợp với hướng dẫn của bên kiểm soát dữ liệu; bên xử lý dữ liệu cũng có thể được yêu cầu sử dụng các biện pháp bảo mật dữ liệu hợp lý, thích hợp và cung cấp cho bên kiểm soát dữ liệu các công cụ cần thiết để thu thập dữ liệu nhằm đáp ứng yêu cầu của các

[2] *Tiêu chuẩn Toàn cầu: Phân biệt giữa Bên kiểm soát và Bên xử lý trong Pháp luật về Bảo mật dữ liệu*, https://www.bsa.org/files/policy-filings/vt03162020controllerprocessor.pdf

chủ thể dữ liệu. Các nghĩa vụ này thường được quy định trong các điều khoản hợp đồng giữa bên kiểm soát dữ liệu và bên xử lý dữ liệu.

Việc kết hợp vai trò của các chủ thể nêu trên như tại Dự Thảo hiện nay gây ảnh hưởng đến một số điều khoản. Mặc dù có sự khác biệt về vai trò và trách nhiệm giữa "bên xử lý dữ liệu cá nhân" và "bên thứ ba" trong một số quy định như "Biện pháp kỹ thuật" (Điều 17) và "Xây dựng quy định bảo vệ dữ liệu cá nhân" (Điều 18), sự khác biệt này là ít rõ ràng hơn ở các điều khoản khác. Điều này bao gồm việc một số nghĩa vụ liên quan đến chủ thể dữ liệu nên được áp đặt lên bên kiểm soát dữ liệu (bên xử lý dữ liệu cá nhân trong Dự Thảo), chẳng hạn như nghĩa vụ phải có được sự đồng ý của chủ thể dữ liệu để xử lý dữ liệu của họ (Điều 8), yêu cầu thông báo cho chủ thể dữ liệu về hoạt động xử lý (Điều 11), khả năng tiết lộ thông tin cá nhân mà không cần sự đồng ý của chủ thể dữ liệu (Điều 6) và nghĩa vụ tôn trọng các yêu cầu về quyền của chủ thể dữ liệu, chẳng hạn như yêu cầu truy cập, xóa hoặc truyền thông tin cá nhân (Điều 5).

Việc thiếu các định nghĩa rõ ràng như hiện tại và sự trùng lặp của các đối tượng này có thể sẽ khiến các chủ thể dữ liệu không thể biết họ nên liên hệ với bên nào để thực hiện quyền đối với dữ liệu cá nhân của họ. Việc người tiêu dùng yêu cầu bên xử lý dữ liệu (bên thứ ba) thực hiện các nghĩa vụ của bên xử lý dữ liệu - các chủ thể mà người tiêu dùng không hay tương tác - tiềm ẩn nhiều rủi ro về an ninh và quyền riêng tư vì hoạt động này buộc bên xử lý dữ liệu (bên thứ ba) đó phải tiết lộ dữ liệu cá nhân tới những cá nhân mà trước đây họ chưa từng có quan hệ trực tiếp và danh tính của các cá nhân này không thể xác định được. Hơn nữa, nhiều bên xử lý dữ liệu (bên thứ ba) theo hợp đồng bị cấm truy cập hoặc xem xét dữ liệu mà họ đang xử lý thay mặt cho khách hàng của họ là bên kiểm soát dữ liệu; việc buộc các bên xử lý (bên thứ ba) truy cập vào dữ liệu cá nhân đó sẽ làm suy yếu các biện pháp bảo vệ quyền riêng tư được thiết lập theo các điều khoản hợp đồng và Dự Thảo.

Cuối cùng, chúng tôi lưu ý rằng việc thiếu các định nghĩa và phân biệt rõ ràng nêu trên là không phù hợp với cách tiếp cận được áp dụng trong pháp luật về quyền riêng tư của các quốc gia khác trên thế giới, chẳng hạn như Quy định Chung về Bảo vệ Dữ liệu của Liên minh châu Âu (**GDPR**),[3] Đạo luật Bảo vệ Dữ liệu Cá nhân (**PDPA**)[4] của Singapore và Đạo luật Bảo vệ Thông tin Cá nhân của Nhật Bản (**APPI**).[5]

Tổng kết lại, **BSA khuyến nghị** những nội dung sau:

- Sửa đổi các định nghĩa tại Điều 2 liên quan đến bên xử lý dữ liệu cá nhân và bên thứ ba để phù hợp với vai trò được chấp nhận phổ biến hơn của bên kiểm soát dữ liệu và bên xử lý dữ liệu.

- Quy định rõ ràng rằng các nghĩa vụ trực tiếp với người tiêu dùng, chẳng hạn như các nghĩa vụ theo Điều 5, 6, 8 và 11 sẽ chỉ áp dụng cho các chủ thể có mối quan hệ trực tiếp với người tiêu dùng, hiện tại trong Dự Thảo là bên xử lý dữ liệu cá nhân (quốc tế gọi là bên kiểm soát dữ liệu).

Tiết lộ Dữ liệu Cá nhân

Điều 6 của Dự Thảo quy định các điều kiện cho phép bên xử lý dữ liệu cá nhân và bên thứ ba tiết lộ dữ liệu và đặt ra năm trường hợp tiết lộ dữ liệu cá nhân mà không cần có sự đồng ý của chủ thể dữ liệu - các trường hợp thường được thể hiện trong các khuôn khổ pháp luật về bảo vệ dữ liệu khác.

Việc thiết lập các cơ chế để tiết lộ dữ liệu cá nhân là rất quan trọng vì điều này cung cấp cho các công ty sự chắc chắn về mặt pháp lý để chuyển dữ liệu cá nhân cho các tổ chức khác cho các hoạt

---

[3] Chỉ thị 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[4] Đạo luật Bảo vệ Dữ liệu Cá nhân 2012, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[5] Đạo luật Bảo vệ Thông tin Cá nhân, https://www.ppc.go.jp/en/legal/

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

động kinh doanh thiết yếu. Tuy nhiên, với ngôn ngữ hiện tại của Điều 6, những trường hợp chuyển giao dữ liệu giữa các chủ thể mà không có sự đồng ý của chủ thể dữ liệu nằm ngoài năm ngoại lệ nêu trên có thể được hiểu là trái phép. Điều này có khả năng làm gián đoạn các hoạt động kinh doanh thiết yếu của doanh nghiệp. Ví dụ: quy định này có thể ngăn cấm việc chuyển dữ liệu cá nhân hợp pháp giữa bên kiểm soát dữ liệu và bên xử lý dữ liệu của họ (bên thứ ba) hoặc giữa các đơn vị kinh doanh trong một công ty.

BSA khuyến nghị rằng Dự Thảo cần đảm bảo rằng dữ liệu cá nhân có thể được tiết lộ vì mục đích và trên cơ sở tương tự mục đích và cơ sở của việc xử lý các dữ liệu cá nhân theo Dự Thảo. Điều này sẽ giúp đảm bảo rằng Điều 6 không ngăn cản việc tiết lộ đối với dữ liệu cá nhân liên quan đến các hoạt động kinh doanh hợp pháp một cách hợp lý nhằm cung cấp sản phẩm hoặc dịch vụ cho chủ thể dữ liệu. Tương tự, Dự Thảo cần làm rõ rằng khi một công ty chuyển dữ liệu cho bên thứ ba xử lý dữ liệu thay mặt công ty đó, thì hành động đó không dẫn đến việc "tiết lộ" cần có sự đồng ý hoặc không phải là ngoại lệ đối với sự đồng ý. Điều này đảm bảo rằng các công ty có thể sử dụng bên xử lý dữ liệu (bên thứ ba) để cung cấp các sản phẩm và dịch vụ mà khách hàng yêu cầu mà không đòi hỏi phải có thêm sự đồng ý bổ sung của người tiêu dùng.

Cơ sở Pháp lý cho Hoạt động Xử lý Dữ liệu Cá nhân

Theo Điều 3, Dự Thảo quy định rằng dữ liệu cá nhân được thu thập và xử lý với sự đồng ý của chủ thể dữ liệu hoặc với sự cho phép của cơ quan có thẩm quyền - Ủy ban BVDLCN. Dự Thảo cũng đưa ra các trường hợp ngoại lệ hạn chế để xử lý dữ liệu mà không có sự đồng ý (Điều 10). Dự Thảo cũng yêu cầu sự đồng ý để xử lý dữ liệu cá nhân bằng các phương tiện, biện pháp tự động (Điều 13) và chuyển dữ liệu cá nhân ra bên ngoài Việt Nam (Điều 21). Dự Thảo cũng có quy định riêng về vấn đề tiết lộ dữ liệu cá nhân (Điều 6).

Các cơ quan quản lý quyền riêng tư và bảo vệ dữ liệu cá nhân trên khắp thế giới từ lâu đã tranh luận về những thách thức và hạn chế của các mô hình bảo vệ dữ liệu cá nhân dựa trên sự đồng ý. Chúng tôi nhận thấy rằng sự đồng ý là cơ sở pháp lý quan trọng cho việc thu thập, sử dụng và tiết lộ thông tin cá nhân. Tuy nhiên, nó không phải là cơ sở pháp lý duy nhất để xử lý dữ liệu cá nhân. Thật vậy, có sự công nhận rộng rãi rằng các khuôn khổ pháp lý dựa trên sự đồng ý có thể làm tăng gánh nặng cho các chủ thể dữ liệu, vì chúng có thể yêu cầu các chủ thể dữ liệu cung cấp sự đồng ý đối với nhiều hình thức xử lý mà họ đã kỳ vọng trước, chẳng hạn như xử lý để cung cấp hàng hóa và dịch vụ mà họ yêu cầu.

Theo đó, chúng tôi khuyến nghị Bộ Công an bổ sung vào Dự Thảo các cơ sở pháp lý khác để xử lý dữ liệu, thay vì dựa vào sự đồng ý làm cơ sở chính để cho phép xử lý dữ liệu.

Đặc biệt, chúng tôi khuyến nghị Bộ Công an sửa đổi Điều 10 để công nhận các căn cứ khác bên cạnh sự đồng ý cho việc xử lý dữ liệu cá nhân — và bằng cách sửa đổi như vậy, công nhận rằng mỗi căn cứ này là cơ sở thích hợp để xử lý dữ liệu chứ không phải là một ngoại lệ trong việc xử lý dữ liệu cá nhân mà không cần sự đồng ý. Cụ thể, Điều 10 cần được sửa đổi để cho phép các trường hợp:

- xử lý dữ liệu cá nhân liên quan đến việc tham gia hoặc thực hiện một hợp đồng với chủ thể dữ liệu;
- thực hiện nghĩa vụ pháp lý mà bên kiểm soát dữ liệu phải tuân theo;
- vì lợi ích hợp pháp mà bên kiểm soát dữ liệu hoặc bên xử lý dữ liệu (bên thứ ba) theo đuổi;[6]
- để bảo vệ lợi ích quan trọng của chủ thể dữ liệu hoặc một thể nhân khác; và

[6] Lợi ích hợp pháp bao gồm xử lý cho các mục đích phát hiện và ngăn chặn lừa đảo; giám sát, phát hiện và bảo vệ mạng thông qua các biện pháp an ninh mạng; và cập nhật các sản phẩm và dịch vụ để đảm bảo rằng chúng chính xác và đáng tin cậy nhất có thể. Vì việc liệt kê phạm vi của những lợi ích hợp pháp này bằng ngôn ngữ luật định là không thực tế, việc sử dụng các căn cứ như "mục đích hợp lý" hoặc "lợi ích hợp pháp" tạo ra sự linh hoạt và chắc chắn về mặt pháp lý cho các công ty để xử lý thông tin cá nhân cho những mục đích hợp pháp này.

- khi việc xử lý là cần thiết để thực hiện một nhiệm vụ vì lợi ích công cộng hoặc để thực thi quyền hạn chính thức được trao cho bên kiểm soát dữ liệu.

Công nhận những cơ sở bổ sung này để xử lý dữ liệu sẽ giúp đảm bảo rằng bên kiểm soát và xử lý dữ liệu (bên thứ ba) có thể sử dụng dữ liệu theo những cách mà người tiêu dùng mong đợi và cho phép họ tăng cường an ninh mạng, để phát hiện và ngăn chặn gian lận cũng như cải thiện quy trình kinh doanh. Hơn nữa, bằng cách công nhận các cơ sở bổ sung để xử lý dữ liệu cá nhân ngoài sự đồng ý, luật bảo vệ dữ liệu cá nhân có thể giảm bớt gánh nặng cho các chủ thể dữ liệu khi họ phải đồng ý cho mỗi lần sử dụng thông tin cá nhân của họ. Khi đó, sự đồng ý được dành cho các tình huống mà có ảnh hưởng nhất đối với chủ thể dữ liệu — khi việc sử dụng có thể liên quan đến thông tin cá nhân nhạy cảm hoặc có thể không mong đợi trong một hoàn cảnh nhất định. Điều này làm giảm "sự mệt mỏi về sự đồng ý" của các chủ thể dữ liệu mà có thể dẫn tới việc cá nhân phớt lờ các thông báo và yêu cầu đồng ý về quyền riêng tư hoặc bị ngăn cản sử dụng các sản phẩm và dịch vụ kỹ thuật số.

Những cơ sở để xử lý dữ liệu này là các đặc trưng được xây dựng hợp lý đã được các khuôn khổ bảo vệ dữ liệu trên toàn cầu đặt ra nhằm tạo điều kiện thuận lợi cho việc sử dụng dữ liệu cá nhân cho các mục đích sáng tạo đồng thời đảm bảo rằng các rủi ro đối với quyền bảo vệ dữ liệu cá nhân được xem xét một cách thích hợp. Các cơ sở này tăng cường bảo vệ dữ liệu cá nhân của các cá nhân trong khi thúc đẩy việc sử dụng dữ liệu cá nhân có trách nhiệm của các doanh nghiệp.

BSA khuyến nghị Bộ Công an sửa đổi Dự Thảo theo hướng bao gồm thêm các cơ sở pháp lý để xử lý dữ liệu như đã nêu. Khi sửa đổi như vậy, những căn cứ này nên được trình bày ở dạng những căn cứ thay thế để xử lý dữ liệu, thay vì ở dạng những ngoại lệ về việc xử lý dữ liệu mà không cần sự đồng ý.

Chuyển Dữ liệu Cá nhân qua Biên giới

Khả năng chuyển giao dữ liệu, bao gồm dữ liệu cá nhân, qua biên giới quốc tế là huyết mạch của nền kinh tế kỹ thuật số hiện đại. Vì lý do này, điều quan trọng là Dự Thảo cho phép các công ty chuyển dữ liệu ra quốc tế một cách có trách nhiệm. Chính phủ Việt Nam đã đồng ý đảm bảo hoạt chuyển giao thông tin xuyên biên giới trong các cam kết quốc tế với các bên của Hiệp định Đối tác Toàn diện và Tiến bộ xuyên Thái Bình Dương.[7]

Chúng tôi quan ngại sâu sắc đối với các yêu cầu hạn chế việc chuyển dữ liệu cá nhân qua biên giới. Theo Khoản 1 Điều 21, dữ liệu cá nhân chỉ có thể được chuyển ra khỏi Việt Nam nếu đáp ứng tất cả các điều kiện sau: a) chủ thể dữ liệu đã đồng ý với việc chuyển dữ liệu; b) “dữ liệu cá nhân gốc” được lưu trữ tại Việt Nam; c) quốc gia mà dữ liệu được chuyển đến áp dụng mức độ bảo vệ dữ liệu tương tự hoặc cao hơn (phải có tài liệu chứng minh); và d) Ủy ban BVDLCN đồng ý với việc chuyển dữ liệu bằng văn bản. Một số yêu cầu này là không thực tế; và khi được áp dụng đồng thời, các yêu cầu này có nguy cơ làm suy yếu khả năng kinh doanh của các công ty toàn cầu tại Việt Nam và đe dọa khả năng hoạt động của các công ty tại Việt Nam trên toàn cầu.

Các công ty trong tất cả các ngành công nghiệp đều đòi hỏi khả năng chuyển dữ liệu qua biên giới quốc tế. Trong các lĩnh vực đa dạng như nông nghiệp, chăm sóc sức khỏe, sản xuất và ngân hàng, các doanh nghiệp sản xuất nhiều loại sản phẩm và dịch vụ, đều có chung nhu cầu gửi dữ liệu qua biên giới quốc tế. Thật vậy, các công nghệ hàng ngày như dịch vụ lưu trữ đám mây, phần mềm quản lý quan hệ khách hàng, chương trình quản lý nguồn nhân lực, dịch vụ quản lý danh tính, phần mềm cộng tác tại nơi làm việc, giải pháp an ninh mạng và dịch vụ quản lý chuỗi cung ứng đều phụ thuộc vào khả năng chuyển giao dữ liệu qua biên giới quốc gia. Hoạt động chuyển giao xuyên biên giới cũng rất quan trọng đối với người tiêu dùng và người lao động - những người mong muốn sử dụng các dịch vụ toàn cầu kết nối họ với những người khác trên toàn thế giới theo cách mà dữ liệu của họ được riêng tư và bảo mật.

Các hạn chế của Điều 21 đối với hoạt động chuyển dữ liệu qua biên giới sẽ làm tổn hại đến khả năng cung cấp dịch vụ toàn cầu của các công ty tại Việt Nam. Hơn nữa, các hạn chế không thúc đẩy các mục tiêu bảo vệ dữ liệu của Dự Thảo. Ví dụ, việc yêu cầu các bản sao dữ liệu cá nhân phải được lưu

[7] Điều 14.11 CPTPP tại https://www.dfat.gov.au/sites/default/files/14-electronic-commerce.pdf

trữ tại Việt Nam sẽ không có tác dụng gì trong việc tăng cường bảo vệ thông tin cá nhân vì tính bảo mật của dữ liệu phụ thuộc vào các chính sách, quy trình và công nghệ mà đơn vị lưu trữ dữ liệu sử dụng, chứ không phụ thuộc vào vị trí thực tế hoặc khu vực tài phán của dữ liệu đó. Ngoài ra, việc yêu cầu Ủy ban BVDLCN phê duyệt trước việc chuyển dữ liệu sẽ gây tốn kém rất nhiều cho Ủy ban BVDLCN và làm gián đoạn các hoạt động kinh doanh thường nhật. Ngay cả yêu cầu đối với các công ty riêng lẻ để xác định xem một khu vực tài phán mà dữ liệu được lưu trữ có đáp ứng mức độ bảo vệ tương đương với mức độ bảo vệ dữ liệu như ở Việt Nam hay không cũng mang tính chủ quan và đòi hỏi nhiều nguồn lực.

Chúng tôi làm rõ dưới đây những quan ngại của chúng tôi đối với các điều kiện có nội hàm rộng, các ngoại lệ hạn hẹp và các kết quả phi thực tế của nghĩa vụ bổ sung được áp đặt lên dữ liệu được chuyển giao.

Các điều kiện có nội hàm rộng: Yêu cầu cả bốn điều kiện phải được thỏa mãn như tại Khoản 1 Điều 21 là không thực tế và có nguy cơ làm mất khả năng hưởng lợi từ các dịch vụ toàn cầu của các công ty, người lao động và người tiêu dùng tại Việt Nam. Chi phí cho việc đảm bảo tuân thủ pháp luật và chậm trễ trong giao dịch đối với đối với các công ty cũng như gánh nặng hành chính đối với Ủy ban BVDLCN là khó để duy trì. Các ngoại lệ được quy định tại Khoản 3 Điều 21 của Dự Thảo cũng không đủ linh hoạt để tạo điều kiện thuận lợi cho việc chuyển dữ liệu.

Chúng tôi khuyến nghị Bộ Công an sửa đổi Điều 21 để tạo thêm sự linh hoạt trong việc chuyển giao dữ liệu qua biên giới.

Các ngoại lệ hạn hẹp: Khoản 3 Điều 21 hiện đưa ra bốn điều kiện để các tổ chức không cần phải đáp ứng các yêu cầu ban đầu nêu trên. Các điều kiện này là: a) chủ thể dữ liệu đồng ý đối với việc chuyển giao; b) Ủy ban BVDLCN có văn bản chấp thuận; c) bên xử lý dữ liệu cá nhân (thuật ngữ này được quốc tế gọi là bên kiểm soát dữ liệu) cung cấp "cam kết bảo vệ dữ liệu cá nhân"; và d) bên xử lý dữ liệu cá nhân cung cấp "cam kết áp dụng các biện pháp bảo vệ dữ liệu cá nhân". Không rõ rằng liệu một tổ chức cần phải đáp ứng một trong các điều kiện nêu trên hay tất cả các điều kiện nêu trên thì mới có thể chuyển giao thông tin cá nhân một cách hợp pháp mà không phải thỏa mãn các nghĩa vụ tại Khoản 1 Điều 21. Bên cạnh đó, các điều kiện tại Điểm a và Điểm b, Khoản 3, Điều 21 dường như nhắc lại các điều kiện tại Điểm a và Điểm d, Khoản 1, Điều 21.

Chúng tôi khuyến khích Bộ Công an sửa đổi Khoản 3 Điều 21 theo hướng quy định rõ rằng việc thỏa mãn một trong hai điều kiện tại Điểm c hoặc Điểm d, Khoản 3, Điều 21 là đủ để chuyển giao dữ liệu cá nhân qua biên giới.

Theo Điểm c và Điểm d, Khoản 3 Điều 21, các công ty có thể chuyển dữ liệu trên cơ sở các cam kết để bảo vệ dữ liệu đó, dù dữ liệu được lưu trữ ở đâu. Các quy định này dường như phản ánh nguyên tắc chịu trách nhiệm, được Tổ chức Hợp tác và Phát triển Kinh tế (**OECD**) [8] thiết lập lần đầu tiên và sau đó đã được thông qua và được tích hợp trong nhiều hệ thống pháp luật bao gồm EU,[9] Nhật Bản,[10] New Zealand,[11] Singapore[12] và Canada.[13] Nguyên tắc chịu trách nhiệm cũng là một đặc điểm quan trọng của Khuôn khổ Quyền riêng tư của APEC,[14] Hệ thống Công nhận Quyền riêng tư của

---

[8] Nguyên tắc chịu Trách nhiệm quy định rằng bên kiểm soát dữ liệu phải chịu trách nhiệm tuân thủ các biện pháp có hiệu lực đối với các nguyên tắc OECD khác bao gồm Nguyên tắc Bảo vệ An Toàn. Khuôn khổ Quyền riêng tư của OECE (trang 15), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[9] Chỉ thị 95/46/EC (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj

[10] Đạo luật Bảo vệ Thông tin Cá nhân (Act on the Protection of Personal Information) của Nhật Bản, https://www.ppc.go.jp/en/legal/

[11] Đạo luật Quyền riêng tư (Privacy Act) 2020 của New Zealand, https://www.legislation.govt.nz/act/public/2020/0031/latest/whole.html#LMS23376

[12] Đạo luật Bảo vệ Dữ liệu Cá nhân (Personal Data Protection Act) 2012 của Singapore, https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act

[13] Các nguyên tắc thông tin công bằng của Đạo luật Tài liệu Điện tử và Bảo vệ Thông tin Cá nhân của Canada, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

[14] Khuôn khổ Quyền riêng tư (Privacy Framework) của APEC, https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

APEC cho các Bên xử lý (**PRP**)[15] và Hệ thống Quy tắc Quyền riêng tư Xuyên Biên giới của APEC (**CBPR**).[16] Theo nguyên tắc này, các tổ chức chuyển dữ liệu trên toàn cầu nên thực hiện các biện pháp để đảm bảo rằng khi dữ liệu được chuyển đến các quốc gia khác với quốc gia nơi dữ liệu được thu thập, dữ liệu sẽ tiếp tục được bảo vệ.

Chúng tôi khuyến nghị Bộ Công an làm rõ rằng việc đáp ứng chỉ Điểm c hoặc Điểm d, Khoản 3 Điều 21 sẽ được coi là đủ để chuyển dữ liệu cá nhân qua biên giới, phù hợp với nguyên tắc chịu trách nhiệm mà chúng tôi đã đề cập ở trên.

Các nghĩa vụ bổ sung không thực tế: Ngoài các điều kiện quá hạn chế đối với việc chuyển dữ liệu xuyên biên giới tại Khoản 1 Điều 21, các quy định trong Khoản 4, 7 và 8 Điều 21 còn đưa ra thêm các yêu cầu nặng nề đối với bên xử lý dữ liệu cá nhân (thuật ngữ này được quốc tế gọi là bên kiểm soát dữ liệu) phải lưu trữ lịch sử chuyển dữ liệu trong ba năm, đăng ký với Ủy ban BVDLCN để chuyển dữ liệu cá nhân nhạy cảm qua biên giới với các yêu cầu đăng ký rất chi tiết và để Ủy ban BVDLCN thực hiện đánh giá hàng năm hoặc các hoạt động giống như kiểm toán đối với hoạt động chuyển dữ liệu qua biên giới của bên xử lý dữ liệu cá nhân. Những nghĩa vụ này là không thực tế và có thể tạo ra những lo ngại mới về quyền riêng tư và bảo mật khi buộc các công ty phải lưu trữ và truy cập dữ liệu mà nếu không bắt buộc thì họ sẽ không làm.

Chúng tôi khuyến nghị Bộ Công an tránh áp đặt các nghĩa vụ như vậy đối với hoạt động chuyển dữ liệu cá nhân qua biên giới.

BSA khuyến nghị các sửa đổi sau đây đối với Điều 21 để tạo điều kiện linh hoạt hơn cho các tổ chức phụ thuộc vào hoạt động chuyển dữ liệu qua biên giới để cung cấp cho các công ty và người tiêu dùng các sản phẩm và dịch vụ, đồng thời đảm bảo mức độ bảo vệ dữ liệu cao:

- Sửa đổi Khoản 1 Điều 21 theo hướng loại bỏ các yêu cầu tại Điểm b, c, và d, Khoản 1 Điều 21 và đồng thời quy định rõ sự đồng ý của chủ thể dữ liệu đối với việc xử lý dữ liệu cá nhân là cơ sở độc lập đủ để cho phép hoạt động chuyển dữ liệu quốc tế.

- Sửa đổi Khoản 1 Điều 21 theo hướng công nhận các cơ sở bổ sung đối với hoạt động chuyển dữ liệu qua biên giới, bao gồm các quy tắc ràng buộc của công ty (*binding corporate rules)*, dấu tin cậy quốc tế *(international trustmarks)*, chứng nhận khu vực và các thỏa thuận hợp đồng. Các cơ chế này được đề cập trong các khuôn khổ pháp lý về bảo vệ dữ liệu khác trên toàn cầu để thúc đẩy các luồng dữ liệu xuyên biên giới, bao gồm các khuôn khổ CBPR và PRP của APEC, GDPR của EU, và APPI của Nhật Bản. Việc công nhận những cơ chế này sẽ giúp Dự Thảo tương thích tốt hơn với các sáng kiến gần đây tại ASEAN, chẳng hạn như xây dựng các Điều khoản Hợp đồng Mẫu của ASEAN[17] và các hoạt động đang diễn ra khác theo Cơ chế Luồng Dữ liệu Xuyên Biên giới của ASEAN.[18]

- Sửa đổi Điểm c và d, Khoản 3 Điều 21 theo hướng làm nổi bật các nghĩa vụ của các công ty (cả bên chuyển dữ liệu và bên nhận dữ liệu) để bảo vệ dữ liệu dù dữ liệu được lưu trữ ở đâu và công nhận rằng các cam kết được thể hiện tại các quy định này là các cơ sở độc lập để chuyển dữ liệu. Như đã trình bày ở trên, cách tiếp cận này phù hợp với nguyên tắc chịu trách nhiệm đã được thực thi theo pháp luật bảo vệ dữ liệu trên thế giới.

[15] Hệ thống Công nhận Quyền riêng tư cho Bên xử lý dữ liệu (Privacy Recognition for Processors) của APEC, http://cbprs.org/wp-content/uploads/2020/08/PRP-Purpose-and-Background-3.pdf

[16] Hệ thống Quy định Quyền riêng tư Xuyên Biên giới (Cross Border Privacy Rules system) của APEC, https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System

[17] Điều khoản Hợp đồng Mẫu của ASEAN về Luồng Dữ liệu Xuyên Biên giới, https://asean.org/storage/3-ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows_Final.pdf

[18] Khuôn khổ Quản lý Dữ liệu của ASEAN, https://asean.org/storage/2-ASEAN-Data-Management-Framework_Final.pdf

- Loại bỏ yêu cầu tại Khoản 4 Điều 21 buộc bên xử lý dữ liệu cá nhân phải lưu trữ lịch sử chuyển dữ liệu trong vòng ba năm. Yêu cầu này có thể dẫn đến các rủi ro ngoài ý muốn về quyền riêng tư và bảo mật do các công ty phải lưu trữ và truy cập vào các dữ liệu mà nếu không bị yêu cầu họ sẽ không làm.

- Loại bỏ yêu cầu đăng ký tại Điểm a, Khoản 7, Điều 21 đối với việc chuyển dữ liệu cá nhân nhạy cảm xuyên biên giới. Bất kỳ yêu cầu nào được quy định tại Dự Thảo đối với việc xử lý dữ liệu cá nhân nhạy cảm (ví dụ như thực hiện báo cáo đánh giá tác động) nên nhắm tới việc xử lý các vấn đề về quyền riêng tư phát sinh từ việc thu thập và sử dụng dữ liệu cá nhân nhạy cảm; tương tự, việc phụ thuộc vào các cơ chế nêu trên của các công ty nhằm mục đích chuyển giao dữ liệu với các biện pháp bảo vệ quyền riêng tư thích hợp sẽ đảm bảo rằng các hoạt động bảo vệ quyền riêng tư vẫn tiếp tục được áp dụng cho dữ liệu, dù dữ liệu đó được lưu trữ ở đâu. Vì vậy, yêu cầu phải đăng ký nêu trên là không thực sự cần thiết.

- Tăng thêm tính linh hoạt đối với các tổ chức theo Khoản 8 Điều 21 bằng cách cho phép các công ty nộp các báo cáo thẩm định độc lập của bên thứ ba và các tài liệu hỗ trợ thay cho việc kiểm tra bổ sung hoặc có tính chất lặp lại được thực hiện bởi Ủy ban BVDLCN.

Điều khoản về Đăng ký

Dự Thảo đặt ra nhiều yêu cầu đăng ký với Ủy ban BVDLCN, bao gồm các yêu cầu đăng ký để xử lý dữ liệu cá nhân nhạy cảm (Điều 20) và để chuyển dữ liệu cá nhân ra bên ngoài Việt Nam (Điều 21). Các yêu cầu này, về bản chất, tương ứng với cơ chế cấp phép xin - cho trên thực tế và dẫn đến sự chậm trễ không cần thiết trong việc xử lý dữ liệu và đi ngược lại với các yêu cầu bảo vệ dữ liệu của hầu hết các quốc gia khác trên thế giới. Các yêu cầu này làm phát sinh các chi phí không cần thiết cho các doanh nghiệp, các nghĩa vụ bổ sung đối với các cơ quan chính phủ khi xem xét và phê duyệt các đơn đăng ký, và không gia tăng sự bảo vệ cho các chủ thể dữ liệu cá nhân. Đó là lý do tại sao Liên minh Châu Âu, ngay cả khi đã tăng cường chế độ bảo vệ dữ liệu của mình trong việc áp dụng GDPR một cách đáng kể, đã loại bỏ hoàn toàn các yêu cầu đăng ký dữ liệu trong Chỉ thị Bảo vệ Dữ liệu được ban hành trước đó.

Trên cơ sở đó, BSA khuyến nghị:

- Loại bỏ các yêu cầu đăng ký tại Điều 20 và Khoản 7, 8 của Điều 21 (các quy định có bản chất áp đặt cơ chế cấp phép xin - cho trên thực tế). Điều này sẽ khuyến khích cả Ủy ban BVDLCN và các doanh nghiệp sử dụng các nguồn lực vốn đã hạn chế cho mục tiêu quan trọng hơn là đảm bảo các kết quả về quyền riêng tư đáng tin cậy cho các chủ thể dữ liệu.

- Sửa đổi các điều khoản liên quan đến các yêu cầu đăng ký nhằm đảm bảo sự nhất quán trong Dự Thảo. Ví dụ, yêu cầu hoạt động xử lý phải được thực hiện đúng với "mục đích đã đăng ký" (Khoản 2 Điều 3) cũng nên được loại bỏ khỏi Dự Thảo.

Yêu cầu về Kỹ thuật

Khoản 1 Điều 17 yêu cầu các tổ chức phải áp dụng nhiều biện pháp hành chính, kỹ thuật và vật lý để bảo vệ dữ liệu cá nhân. Tuy nhiên, không phải tất cả các yêu cầu này đều phù hợp với mọi tổ chức xử lý thông tin cá nhân. Do đó, chúng tôi đề nghị Bộ Công an làm rõ rằng các biện pháp chỉ cần được áp dụng "khi thích hợp"[19] và không bắt buộc phải được thực hiện bởi tất cả các bên kiểm soát dữ liệu trong mọi trường hợp.

Ngoài ra, **BSA đề xuất** Bộ Công an không áp đặt các phương pháp tiếp cận bảo mật bắt buộc, và thay vào đó, khuyến nghị Bộ Công an áp dụng phương pháp tiếp cận linh hoạt, trung lập về công nghệ, dựa trên rủi ro để bảo vệ dữ liệu cá nhân - cách tiếp cận phù hợp với các tiêu chuẩn và thực tiễn tốt nhất được quốc tế công nhận. Ví dụ, Điểm g, Khoản 2 Điều 17 yêu cầu bên xử lý dữ liệu cá nhân phải lưu trữ thông tin về loại thiết bị và phần mềm được sử dụng để xử lý dữ liệu cá nhân.

[19] Vui lòng xem Điều 32, GDPR của Liên minh Châu Âu

Thông tin này không góp phần vào việc đảm bảo an toàn hoặc xử lý dữ liệu có trách nhiệm và BSA khuyến nghị nên loại bỏ yêu cầu này.

Dữ liệu Cá nhân Nhạy cảm

Định nghĩa hiện tại về dữ liệu cá nhân nhạy cảm tại Khoản 3 Điều 2 có nội hàm rộng một cách không cần thiết. Định nghĩa bao gồm các danh mục dữ liệu đặc biệt,[20] cũng như dữ liệu tài chính, dữ liệu vị trí cá nhân và dữ liệu cá nhân về các mối quan hệ xã hội. Định nghĩa này cũng không giới hạn cụ thể các loại dữ liệu nhạy cảm này ở dữ liệu rõ ràng được dùng để xác định một chủ thể hoặc có thể sử dụng để xác định danh tính của chủ thể dữ liệu. Điều này dẫn đến việc quy định này có thể bao hàm những nội dung vượt quá phạm vi thông tin cá nhân.

BSA khuyến nghị Bộ Công an sửa đổi định nghĩa nêu trên để đảm bảo phù hợp hơn với các tiêu chuẩn quốc tế về dữ liệu cá nhân nhạy cảm và đặc biệt là giới hạn điều khoản này ở dữ liệu rõ ràng được dùng để xác định một chủ thể hoặc có thể sử dụng để xác định danh tính của chủ thể dữ liệu.

Xử phạt và Bồi thường

Cơ quan quản lý nên có các công cụ và nguồn lực cần thiết để đảm bảo việc thực thi pháp luật hiệu quả. Việc thực thi pháp luật bảo vệ dữ liệu cá nhân một cách hiệu quả rất quan trọng trong việc bảo vệ quyền riêng tư của người tiêu dùng, đảm bảo rằng các tổ chức thực hiện những cam kết và nghĩa vụ pháp lý của họ và giúp ngăn ngừa những hành vi vi phạm tiềm tàng. Pháp luật bảo vệ dữ liệu cá nhân có thể tạo ra sự thực thi hiệu quả mà không cần đưa ra các hình phạt hình sự hoặc bao gồm quyền khởi kiện của cá nhân.

Các biện pháp xử lý và hình phạt áp dụng cho các hành vi vi phạm pháp luật bảo vệ dữ liệu cá nhân nên được quy định tương ứng với mức độ thiệt hại gây ra bởi các hành vi vi phạm đó. Hình phạt hình sự không tương xứng với các biện pháp xử lý trong trường hợp này.

Vì vậy, **BSA khuyến nghị** rằng Bộ Công an sửa đổi Khoản 1 Điều 4 theo hướng loại bỏ các quy định đề cập đến các hình phạt hình sự.

Điều 5 quy định rằng các chủ thể dữ liệu có quyền khiếu nại nếu dữ liệu cá nhân của họ bị xâm phạm hoặc xử lý không chính xác hoặc việc thực hiện quyền đối với dữ liệu cá nhân của họ không được áp dụng một cách chính xác. Quy định này cũng trao quyền yêu cầu bồi thường khi có "căn cứ cho rằng dữ liệu cá nhân của mình bị xâm phạm" cho các chủ thể dữ liệu.

Việc quy định cho người tiêu dùng quyền khởi kiện sẽ tạo ra sự thiếu chắc chắn không cần thiết về cách thức thực thi pháp luật bảo vệ dữ liệu cá nhân. Việc trao quyền năng thực thi pháp luật vào một cơ quan chính phủ, ví dụ như Ủy ban BVDLCN như theo Dự Thảo, sẽ tạo ra khả năng thực thi pháp luật một cách hiệu quả và nhất quán, đồng thời tạo cho các tổ chức và người tiêu dùng sự chắc chắn về cách áp dụng các quyền và nghĩa vụ quy định trong Dự Thảo.

Theo đó, **BSA khuyến nghị** rằng Bộ Công an giới hạn Khoản 5 Điều 5 trong phạm vi khiếu nại tới Ủy ban BVDLCN và loại bỏ Khoản 6 Điều 5 trong Dự Thảo.

[20] Vui lòng xem Điều 9, GDPR của Liên minh Châu Âu.

300 Beach Road
#25-08 The Concourse
Singapore 199555
P +65 6292 2072
F +65 6292 369
W bsa.org
Regional Representative Office
UEN: S97RF0005K

Một lần nữa, BSA gửi lời cảm ơn tới Chính phủ Việt Nam đã thực hiện bước tiến quan trọng trong việc xây dựng một cơ chế quốc gia về bảo vệ dữ liệu và lời cảm ơn tới Bộ Công an đã tạo cơ hội cho chúng tôi được đóng góp ý kiến đối với các điều khoản trong Dự Thảo. Nếu Bộ Công an cần giải thích bất cứ nội dung hay cần thêm thông tin nào liên quan đến thư này, vui lòng liên hệ với người ký tên dưới đây tại brianf@bsa.org hoặc +65 8328 0140.

Trân trọng,



Brian Fletcher
Giám đốc Chính sách - Khu vực Châu Á - Thái Bình Dương
BSA | Liên minh Phần mềm